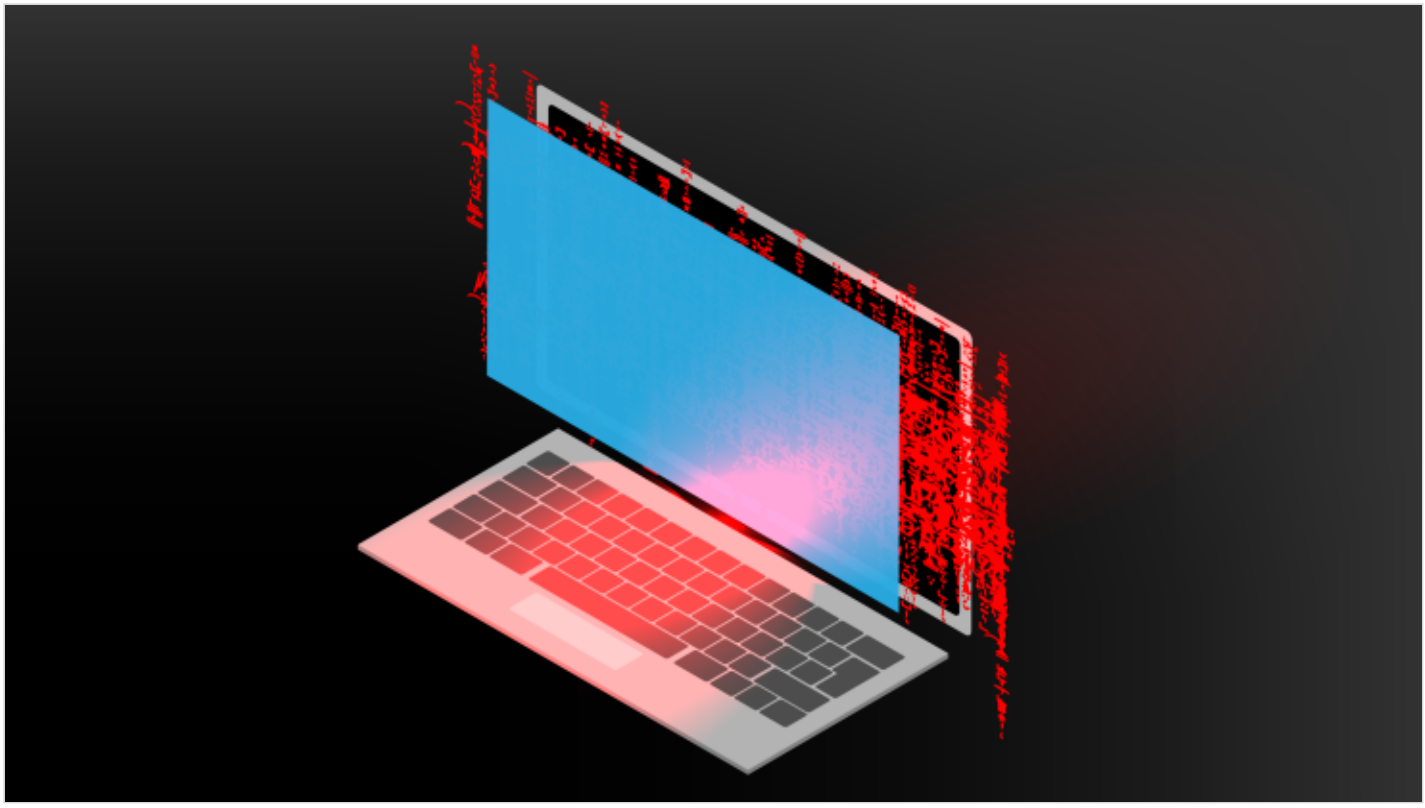
Cryptojacking attack hits ~4,000 websites, including UK's data watchdog

Posted Feb 12, 2018 by Natasha Lomas (@riptari)



At first glance a CoinHive crypto miner being served by a website whose URL contains the string 'ICO' might not seem so strange.

But when you know that ICO in this case stands for the UK's Information Commissioner's Office — aka the national data protection and privacy watchdog, whose URL (https://ico.org.uk) predates both Bitcoin and the current craze for token sales — well, the extent of the cryptojacking security snafu quickly becomes apparent.

Nor is the ICO the only website or government website caught serving cryptocurrency mining malware to visitors on every page they visited. Thousands of sites were compromised via the same plugin.

Security researcher Scott Helme flagged the issue via Twitter yesterday, having been initially alerted by another security professional, Ian Trump.

Helme traced the source of the infection to an accessibility plugin, called Browsealoud, created by a UK company called Texthelp.

The web screen reader software was being used on scores of UK government websites — but also further afield, including on government websites in the US and Australia.

So when an attacker injected a crypto mining script into Browsealoud's JavaScript library some 4,000 websites — a large number of them taxpayer funded and/or subsidized — were co-opted into illegal crypto mining… Uh, oopsie…

tl;dr: "If you want to load a crypto miner on 1,000+ websites you don't attack 1,000+ websites, you attack the 1 website that they all load content from," as Helme has since blogged about the attack.

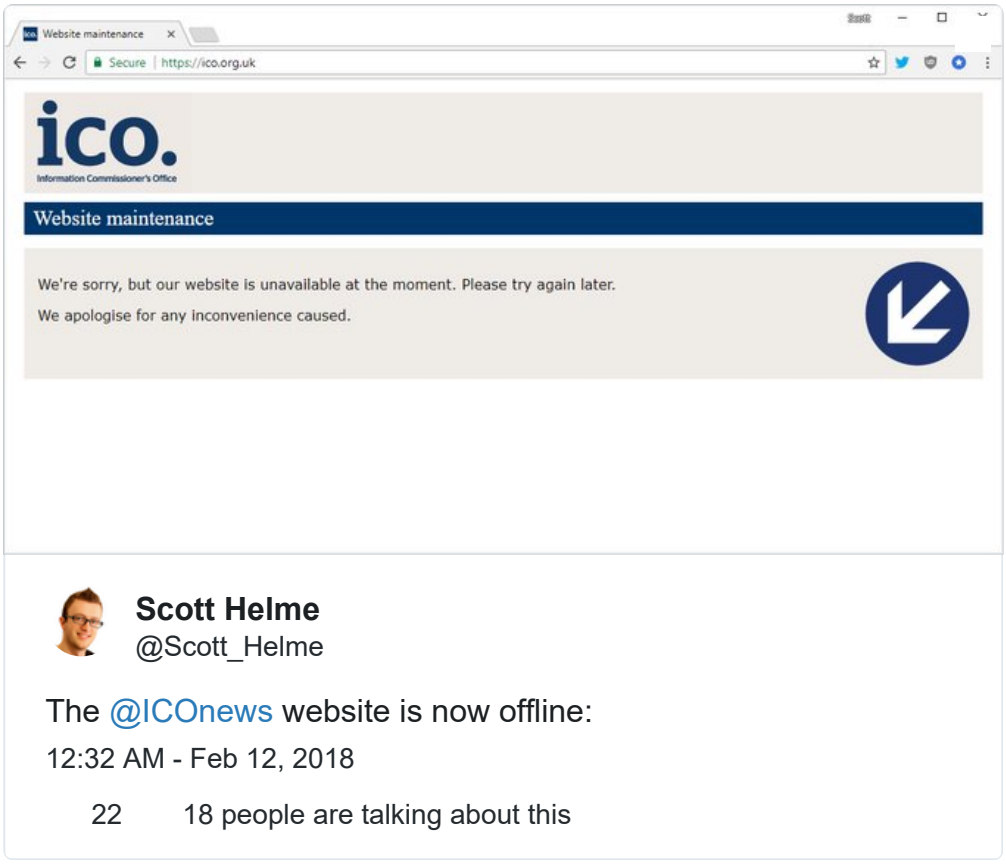
Texthelp has also since issued a statement — confirming it was compromised by (as yet) unknown attackers, and saying it is investigating the incident.

"At 11:14 am GMT on Sunday 11th February 2018, a JavaScript file which is part of the Texthelp Browsealoud product was compromised during a cyber attack," it writes. "The attacker added malicious code to the file to use the browser CPU in an attempt to illegally generate cryptocurrency. This was a criminal act and a thorough investigation is currently underway."

According to Texthelp the crypto miner was active for four hours on Sunday — before, the company claims, its own "continuous automated security tests" detected the modified file in Browsealoud and responded by pulling the product offline.

"This removed Browsealoud from all our customer sites immediately, addressing the security risk without our customers having to take any action," it further claims.

However, at the time of writing, the ICO's website remains down for "website maintenance" — having been taken offline on Sunday soon after Helme raised the alert.



We reached out to the ICO with questions and a spokesperson responded with this statement: "We are aware of the issue and are working to resolve it. We have taken our website down as a precautionary measure whilst this is done."

The spokesman added that the ICO's website remains offline today because it's investigating what it believes is another Browsealoud-associated issue.

"The ICO's website will remain closed as we continue to investigate a problem which is thought to involve an issue with the Browsealoud feature," the spokesperson told us, without elaborating further.

Yesterday the UK's National Cyber Security Center issued its own statement about the crypto miner attack, writing:

> *NCSC technical experts are examining data involving incidents of malware being used to illegally mine cryptocurrency.*
>
> *The affected service has been taken offline, largely mitigating the issue. Government websites continue to operate securely.*

> *At this stage there is nothing to suggest that members of the public are at risk.*

Texthelp has also claimed that no customer data was "accessed or lost" as a result of the attack, saying in its statement yesterday that it had "examined the affected file thoroughly and can confirm that it did not redirect any data, it simply used the computers CPUs to attempt to generate cryptocurrency".

We've also reached out to Texthelp for any updates on its investigation — at the time of writing the company has not responded.

But even if no user data has indeed been compromised, as it's claiming, the bald fact that government websites were found to be loading a CoinHive crypto miner which clandestinely and thus illegally mined cryptocurrency en mass is hugely embarrassing. (Albeit, as Helme points out, the attack could have been much, much worse. A little CPU burn is not, for e.g., stolen credit card data.)

Still, Helme also argues there is added egg-on-face here — perhaps especially for the ICO, whose mission is to promote data protection best practice including robust digital security — because the attack would have been trivially easy to prevent, with a small change to how the third party JS script was loaded.

In a blog post detailing the incident he describes a method that would have mitigated the attack — explaining:

> *What I've done here is add the **SRI Integrity Attribute** and that allows the browser to determine if the file has been modified, which allows it to reject the file. You can easily generate the appropriate script tags using the **SRI Hash Generator** and rest assured the crypto miner could not have found its way into the page. To take this one step further and ensure absolute protection, you can use **Content Security Policy** and the **require-sri-for** directive to make sure that no script is allowed to load on the page without an SRI integrity attribute. In short, this could have been totally avoided by all of those involved even though the file was modified by hackers. On top of all of that, you could be alerted to events like this happening on your site via **CSP Reporting** which is literally the reason I founded **Report URI**. I guess, all in all, we really shouldn't be seeing events like this happen on this scale to such prominent sites.*

Although he does also describe the script the ICO used for loading the problem JS file as "pretty standard".

So it does not look like the ICO was doing anything especially unusual here — it's just that, well, a national data protection agency should probably be blazing a trail in security best practice,

rather than sticking with riskier bog standards.

Not to single out the ICO too much though. Among the other sites compromised in the same attack were US courts, the UK's financial ombudsman, multiple local government websites, National Health Service websites, higher education websites, theatre websites and Texthelp's own website, to name a few.

And with volatile cryptocurrency valuations clearly incentivizing cryptojacking, this type of malware attack is going to remain a problem for the foreseeable future.

Also blogging about the incident, and the SRI + CSP defense proposed by Helme, web security expert Troy Hunt (of haveibeenpwned.com data breach search service fame) has a bit more of a nuanced take, pointing out that third party plugins can be provided as a service, rather than a static library, so might need (and be expected) to make legitimate changes.

And therefore that the wider issue here is how websites are creating dependencies on external scripts — and what can be done to fix that. Which is certainly more of a challenge.

Perhaps especially for smaller, less well-resourced websites. At least as far as government websites go, Hunt argues they should definitely should be doing better in shutting down these types of web security risks.

"They *should* be using SRI and they *should* be only allowing trusted versions to run. This requires both the support of the service (Browsealoud) not to arbitrarily modify scripts that subscribers are dependent on *and* the appropriate processes on behalf of the dev teams," he writes, arguing that government websites need to take these risks seriously and have a prevention plan incorporated into their software management programs — as standard.

"There are resources mentioned above to help you do this — retire.js is a perfect example as it relates to client-side libraries," he adds. "And yes, this takes work."

But if the ICO isn't going to do the work to lock down web application risks, how can the national data watchdog expect everyone else to?

Phil Ashby @PhlashGBG 12 Feb

Replying to @troyhunt @Scott_Helme

Much as CSP & SRI may have helped, that makes /ongoing work/ for all the site authors, which they don't wanna do, that's why they outsourced their problems to start with... why have script block signature initiatives been dropped, did everyone think one TLS perimeter was enough?

Troy Hunt
@troyhunt

Is the tl;dr that good security takes some planning? If so, yes, I agree 😀

8:00 AM - Feb 12, 2018 · Gold Coast, Queensland

2 See Troy Hunt's other Tweets

FEATURED IMAGE: BRYCE DURBIN

FEATURED STORIES

Self Driving Porsche Powered by Huawei's Mate 10 Pro
VIDEO | 1:57 | GADGETS

Blockchain will work in trucking — but only if these three things happen
14 HOURS AGO | JONATHAN SALAMA

UiPath raising around $120M at $1B+ valuation for its 'software robots' for internal business tasks
15 HOURS AGO | INGRID LUNDEN, STEVE O'HEAR

Alexa has literally lost her voice as users report outages and unresponsiveness
18 HOURS AGO | FITZ TEPPER

MIT study shows how much driving for Uber or Lyft sucks
19 HOURS AGO | NATASHA LOMAS

LATEST FROM EUROPE

UiPath raising around $120M at $1B+ valuation for its 'software robots' for internal business tasks

15 HOURS AGO | INGRID LUNDEN, STEVE O'HEAR

Facebook's wider Kremlin Brexit ad sweep draws a blank

18 HOURS AGO | NATASHA LOMAS

MIT study shows how much driving for Uber or Lyft sucks

19 HOURS AGO | NATASHA LOMAS

Angry Birds maker Rovio misses Q4 on sales of €73.9M, EPS of €0.10, closes London studio

YESTERDAY | INGRID LUNDEN

About

Staff

Contact Us

Advertise With Us

Event & Editorial Calendar

Send Us A Tip

Activations Blog

International

China

Europe

Japan

Follow TechCrunch

TechCrunch Apps

The Daily Crunch

Latest headlines delivered to you daily

Enter Email Address SUBSCRIBE